Notice of Allowability	Application No.	Applicant(s)	
	10/659,129	THERRIEN ET AL.	
	Examiner	Art Unit	
	CHARLES D. ADAMS	2164	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *After Final amendment of 8 November 2010*.

2. ☒ The allowed claim(s) is/are *1,3-5,7-17 and 19-26*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date *11-20-2010* .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

EXAMINER'S AMENDMENT

Remarks

1. In response to communications filed on 8 November 2010, claims 1, 3-5, 7, and 17 are amended. Claims 1, 3-5, 7-17, and 19-26 are pending in the application.

Amendments to the Claims

2. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Boris Matvenko (Reg. No. 48,165) on 19 November 2010.

In Claims:

1. (**Currently Amended**). A data protection system, comprising:

a fileserver configured to contain shares of data and to be in communication with at least one local repository that is in communication with at least one remote repository, wherein two or more repositories are configured to store a replica of a file, wherein each repository includes multiple repository nodes, at least one repository node of each repository is configured to store the replica of the file, wherein a storage location

and a number of replicas in each repository is configured to be changed over time by a user;

wherein based on a criticality of the file, the number of stored replicas of the file is increased or decreased in at least one repository;

wherein shares of data are directories or folders of storage capacity created on the fileserver;

the fileserver includes:

a filter driver ~~operative~~ configured to intercept input or output activity initiated by client file requests, including modification of any existing stored files and[[/or]] creation of new files as ~~they~~ modification of any existing stored files and creation of new files occur, and further configured to capture a snapshot of a set of the shares of data at a particular point in time and to maintain a list of modified and[[/or]] created files since a last snapshot occurred;

a file system in communication with the filter driver and ~~operative~~ configured to store client files;

the fileserver is configured to store a unique protection policy for each share of data on the fileserver, the protection policy defines:

repositories used to protect each share of data;

frequency of data protection;

number of replicas of each file that are maintained in each repository; and,

maintenance of modifications to each share of data;

based on the definitions in the protection policy, the filter driver is configured to capture the snapshot.

2. (Cancelled).

3. (**Currently Amended**). The system of claim 1, wherein the fileserver further comprises:

a location cache configured to determine based on the protection policy which repository will be used to protect each share of data; and

a location manager coupled to the location cache and ~~operative~~ configured to update the location cache when the fileserver protects a new share of data in a specific repository node.

4. (**Currently Amended**). The system of claim 3, wherein the local repository in communication with the fileserver is adapted for receiving files from the fileserver;

the local repository is further ~~adapted~~ configured to receive replicated files from the fileserver; and

the local repository includes a protection policy component ~~operative~~ configured to determine whether new versions of existing files should be compressed and whether older versions of existing files should be maintained.

5. (**Currently Amended**). The system of claim 4, wherein the remote repository in communication with the local repository is adapted for receiving files from the local repository;

the remote repository is further ~~adapted~~ configured to receive replicated files from the local repository; and

the remote repository includes a protection policy component configured to determine whether new versions of existing files should be compressed and whether older versions of existing files should be maintained.

6. (**Cancelled**).

7. (**Currently Amended**). A method for protecting data comprising:

providing a fileserver configured to contain sets of files and to be in communication with at least one local repository that is in communication with at least one remote repository, wherein two or more repositories are configured to store a replica of a file;

wherein sets of files are directories or folders of storage capacity created on the fileserver;

the fileserver including

a filter driver configured to intercept input or output activity initiated by client file requests, including modification of any existing stored files and creation of new files as modification of any existing stored files and creation of new files occur;

a file system in communication with the filter driver and operative to store client files;

storing a version of a file within a set of files on ~~a primary disk storage system~~ the fileserver;

using the filter driver, capturing a snapshot of the set of files at a particular point in time based on a backup frequency defined in a protection policy;

using the filter driver, maintaining a list of modified and[[/or]] created files since last captured snapshot;

examining the protection policy associated with the set of files to determine where and how to protect files associated with the set of files;

wherein the protection policy defines:

repositories used to protect each ~~share of data~~ set of files;

frequency of data protection;

number of replicas of each file that are maintained in each repository; and,

maintenance of modifications to each ~~share of data~~ set of files;

and,

replicating the version of the file to two or more repositories specified by the protection policy, wherein the repositories include at least one ~~of a~~ local repository and at least one remote repository, wherein a storage location and a number of replicas of the version of the file is configured to be changed over time by a user;

wherein each repository includes multiple repository nodes, at least one repository node of each repository is configured to store the replica of the file;

wherein based on the criticality of the file, the number of stored replicas of the file is increased or decreased in at least one repository;

wherein the protection policy is configured to be uniquely defined for each set of files.

8. (Previously Presented). The method of claim 7 wherein the file is configured to have at least one version.

9. (Previously Presented). The method of claim 8 wherein the method further comprises:

applying reverse delta compression to the version of the file when a successive version of the file is stored in the repository.

10. (Previously Presented). The method of claim 9 wherein the step of applying reverse delta compression comprises

creating another version of the file, wherein the another version of the file is a version of the file successive to the version of the file;

replicating the another version of the file into the local repository and the remote repository;

replacing the replicated version of the file in the local repository with a reverse delta compressed version representing a difference between the version of the file and the another version of the file and replicating;

transmitting the reverse delta compressed version to the remote repository; and

in the remote repository, replacing the version of the file with the reverse delta compressed version to store the another version and the reverse delta compressed version.

11. (Previously Presented). The method of claim 7 wherein examining a protection policy associated with the set of files to determine where and how to protect files associated with the set of files comprises:

determining the location of repositories and a number of replicas of the files to be stored in each repository.

12. (**Currently Amended**). The method of claim 7 wherein examining a protection policy associated with the set of files to determine where and how to protect files associated with the set of files comprises:

determining whether to purge [[a]] the file from a repository after the file has been deleted from a set of files.

13. (Previously Presented). The method of claim 7 wherein examining a protection policy associated with the set of files to determine where and how to protect files associated with the set of files comprises:

determining whether to keep a version history of a file in the set of files.

14. (Previously Presented). The method of claim 7 wherein examining a protection policy associated with the set of files to determine where and how to protect files associated with the set of files comprises:

determining a specified backup frequency for a repository.

15. (Previously Presented). The method of claim 7 wherein examining a protection policy associated with the set of files to determine where and how to protect files associated with the set of files comprises:

determining a specified type of compression for a file in the set of files.

16. (Previously Presented). The method of claim 7 wherein examining a protection policy associated with the set of files to determine where and how to protect files associated with the set of files comprises:

determining a specified caching level of a repository.

17. (**Currently Amended**). A data protection system comprising:

a fileserver configured to contain shares of data and to be in communication with at least one local repository that is in communication with at least one remote repository, wherein two or more repositories are configured to store a replica of a file, wherein each repository includes multiple repository nodes, at least one repository node of each repository is configured to store the replica of the file, wherein a storage location and a number of replicas in each repository is configured to be changed over time by a user;

wherein based on a criticality of the file, the number of stored replicas of the file is increased or decreased in at least one repository;

wherein shares of data are directories or folders of storage capacity created on the fileserver;

said fileserver includes:

filter driver means for intercepting input or output activity initiated by client file requests, including modification of any existing stored files and[[/or]] creation of new files as ~~they~~ modification of any existing stored files and creation of new files occur, and for capturing a snapshot of a set of the shares of data at a particular point in time and for maintaining a list of modified and[[/or]] created files since a last snapshot occurred;

file system means in communication with the filter driver, the file system means for storing client files;

the fileserver is configured to store a unique protection policy for each share of data on the fileserver, the protection policy defines:

repositories used to protect each share of data;

frequency of data protection;

number of replicas of each file that are maintained in each repository; and,

maintenance of modifications to each share of data;

based on the definitions in the protection policy, said filter driver means is configured to capture the snapshot.

18. (Cancelled).

19. (Previously Submitted). The system of claim 1, wherein said fileserver is configured to

backup said modified files into repositories identified in said protection policy based on said backup frequency; and

store a latest version of a file in a repository where a prior version of said file is stored;

determine a difference between said latest version of said file and said prior version of said file;

apply reverse delta compression to said difference;

replace said prior version of said file with said reverse delta compressed difference between said latest version and said prior version of said file.

20. (Previously Submitted). The system of claim 1, wherein, based in the protection policy, the fileserver is configured to determine the location of repositories and a number of replicas of the files to be stored in each repository.

21. (Previously Submitted). The system of claim 1, wherein, based on the protection policy, the fileserver is further configured to determine whether to purge a file from a repository after the file has been deleted from a set of files.

22. (Previously Submitted). The system of claim 1, wherein, based on the protection policy, the fileserver is further configured to determine whether to keep a version history of a file in the set of files.

23. (Previously Submitted). The system of claim 1, wherein, based on the protection policy, the fileserver is further configured to determine a specified backup frequency for a repository.

24. (Previously Submitted). The system of claim 1, wherein, based on the protection policy, the fileserver is further configured to determine a specified type of compression for a file in the set of files.

25. (Previously Submitted). The system of claim 1, wherein, based on the protection policy, the fileserver is further configured to determine a specified caching level of a repository.

26. (Previously Submitted). The system of claim 17, wherein the fileserver further includes

backup means for backing up the modified files into repositories identified in the protection policy based on the backup frequency;

storage means for storing a latest version of a file in a repository where a prior version of the file is stored;

means for determining a difference between the latest version of the file and the prior version of the file;

means for applying reverse delta compression of the difference; and

means for replacing the prior version of the file with the reverse delta compressed difference between the latest version and the prior version of the file.

Reasons for Allowance

3. The following is an examiner's statement of reasons for allowance:

The prior art of record does not show the features of the independent claims, nor would the features of the independent claims have be obvious to one of ordinary skill in the art at the time the invention was made upon considering the cited references.

Specifically, the prior art of record does not show a unique protection policy according to the four claimed elements for each share of data on the file server, wherein each share of data has a unique protection policy, along with a filter driver that performs according to the independent claims, operating in a system with the particular arrangement of repositories and nodes wherein the number of copies of a particular file is increased or decreased according to the criticality of the file.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

4. Any inquiry concerning this communication or earlier communications from the examiner should be directed to CHARLES D. ADAMS whose telephone number is (571)272-3938. The examiner can normally be reached on 8:30 AM - 5:00 PM, M - F.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Charles Rones can be reached on (571) 272-4085. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/C. D. A./
Examiner, Art Unit 2164

/Charles Rones/
Supervisory Patent Examiner, Art Unit 2164